Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1242 10/15/10

~ Oz PM Backs Web Filter ~ People Are Talking! ~ New Firefox Trojan!
~ New Norton 360 in Beta ~ Oracle Pledges Support! ~ Star Raiders Revival!
~ US Still #1 in Botnets ~ MS Scared of OpenOffice ~ Keyed Laptop Lock!

~ Yahoo Buyout Rumors! ~ Webcam Spy Case Settled ~ New Mac OS Coming?

-* MS Looks to Courts vs Botnets *-
-* UK Hit by 1000 Cyber Attacks Monthly *-
-* MS Releases Biggest-Ever Security Update! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Unless you've been living in a cave (pun intended) for the past couple of months, the best "touchy-feely" news of the day is recovery of the miners that were trapped in a collapsed mine in Chile for over two months. It's truly amazing that these miners were located, alive, over a half mile below the surface of the earth - and freed, one at a time. To watch some of those miners getting out of the "capsule" in such great condition was awe-inspiring. With all of the tragedies and negative news permeating the airwaves lately, this rescue effort was certainly something to witness.

I'm sure that we'll hear more details of the entire ordeal over the next few months, and will continue to be amazes. And yes, there will certainly be a book or three; and you just know that a movie will be in the works. But, this is the type of story that warrants such endeavors. While I hope that all of these miners' lives return to some normalcy, you have to wonder what their lives will be like moving forward. Hopefully, the world will soon let them have time to recover and resume their lives. What a great story!

Until next time...

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

Hidi ho, friends and neighbors. Well, I guess the big news all over the world is those Chilean miners. Hey, it IS amazing that they've all been saved, and it's a great story.

Imagine being stuck underground for more than 2 months in 90 degree heat without enough food, water or light. And imagine being alive after those 70 or so days and waiting your turn to be shuttled up to the surface again.

All in all, it's an amazing story. And, if I understand it correctly, one of the reasons that the miners ended up safe was because it was a copper mine, not a coal mine. With coal, there's always (I guess) a lot of

poisonous and/or flammable gas. It’s the nature of the beast. With copper and other metals, there can still be pockets of gas and such, but it’s much less likely to be the problem it is with coal.

Of course, it’s a source of national pride for Chile, of personal pride for the miner and their families and friends, and for everyone who helped out in the rescue operation.

I guess there’s more I could say about the Chilean miners, but is there really anything I can tell you that you haven’t already heard a dozen times? Yeah, I didn’t think so.

So what else to talk about...

Oh, how about that newly discovered planet, Gliese 581g? Now here’s a big story, right? A world "about" the size of the earth, circling around a star only about six trillion miles from us. That’s about 20 light years; in our own back yard, by cosmic standards. We’ll talk a little bit more about the importance of shorter distances in a bit.

Now, the discoverers of this new world figure that the planet has somewhere between three and four times the mass of the earth, so it’s probably a rocky, or ’terrestrial’ planet like the Earth, Mars, Venus and Mercury. Most people who seem to know what they’re talking about figure that after a certain size, a planet’s gravity will accumulate debris and gas floating around in space and form a thick, almost liquid atmosphere like Jupiter and Saturn or even larger to become a brown dwarf. So if Gliese 581g is 3 to 4 times the mass of the Earth (that’s MASS, not radius), it’s large enough to keep an atmosphere but small enough that it’s not going to become a gas giant.

Now the reason that I emphasized that this planet is 3 to 4 times the MASS of the Earth bears some explanation for a pretty good reason. If we take for granted that this planet is composed of the same stuff that the Earth is, it would have the same mass if it were the same SIZE as the Earth. But that’s not the case here. Let’s say that the the planet weighs in on the low side at ’only’ 3 times the mass of the Earth. Now that doesn’t mean that it would be three times the radius of the Earth.

Let’s say that Gliese 581g has three times the mass of the Earth. That doesn’t mean that it’ll be three times the radius of the Earth. If everything else was equal, it’d only be about about a third ’bigger’ than the Earth. This becomes important for another reason... Gravity.

Most people think of gravity as being "in effect" at the surface of the Earth... on the ground. But the fact is that gravity is "in effect" right from the center of gravity itself. If you’re talking about just the Earth, then its right at the very center of the Earth that gravity ’starts’.

This has some interesting implications which we should think about. The ’strength’ of gravity decreases by the inverse square of the distance from the center of gravity. Without doing all the math (never my strong suit), gravity on a planet that’s about 3 times the mass of the earth, which would be about a third larger from "side to side", would be a little less than three times Earth’s gravity. Still formidable, but it’s not impossible to imagine. A 100 pound person would weight a little bit less than 300 pounds if standing on this newly discovered world.

Now, Gliese 581g orbits its star much closer than the Earth orbits the sun. Instead of taking a year to make one complete orbit like the Earth

does, Gliese 581g takes about 37 days. If the Earth was that close to the sun (about half the distance from the sun to the planet Mercury), the oceans would have boiled off, the atmosphere burned away, and it would be a barren rock. But since its star is a red dwarf start; a smaller, dimmer, cooler star than the sun, this distance is right in the "Goldilocks Zone". It’s not too cold, and not too hot.

But there’s one slight problem with a planet being this close to its star: It becomes ’tidally locked’... one side of the planet will always face the star, one side will always be in darkness.

It’s the same as our moon. It rotates at the same rate as it orbits its mutual center of gravity with the Earth, so the same side is always facing us. By the way, there is no ’dark side’ of the moon. What we think of as the dark side actually gets more sun than "our" side, since the Earth’s shadow blocks some of the sunlight when it’s between the sun and moon.

So we have a large planet that could possibly have an atmosphere and liquid water, but is tidally locked. Does this mean that one side is too hot and the other too cold? It might. But it could also be that the atmosphere would transfer heat from the day side to the night side or that the ’fringes’ of the day side could be ’just right’. We’ll have to wait to see.

Now the most interesting thing here is that the planet is ’only’ 20 light years from Earth. That means that if we sent a radio signal to it, it would take 20 years to reach it. If there were indeed intelligent beings with the technology to send and receive radio signals, and if they could decode ours and reply, it would ’only’ take 40 years to find out.

Of course, no one is holding out much hope for that, but it might make us wonder about other worlds around other planets about the same distance away.

Ah, but there’s yet another twist when dealing with Gliese 581g... it might not even be there! Another team of scientists have looked at some of the data and have said that they don’t see evidence for a planet ’g’ at all!

I guess time will tell. At this point I’m not even sure that we could prove that the EARTH exists or, if it does, that there’s intelligent life there. [grin]

That’s all for this week, folks. Tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week’s Gaming Section - ’Medal of Honor’ Hits Stores!
  """"""""""""""""""""""""""""""" Atari Revives Star Raiders!
  ’Ironclad’ Gaming Mouse Mat!
  And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""

'Medal of Honor' Hits Stores, Takes Battle to Afghanistan

Electronic Arts's highly anticipated "Medal of Honor" hit stores on Tuesday, with the newest version of the popular video game set in war-torn Afghanistan.

The latest release is the first time that the 11-year-old, first-person shooter game has left its traditional World War II setting.

"'Medal of Honor' is an authentic look into today's war," said Greg Goodrich, the game's executive producer, said earlier this year. "Inspired by real people and real events, the game puts players in the boots of today's warrior, from the infantry ground pounder to the Tier 1 Operator."

EA said "unprecedented access to the U.S. Army," added to its realistic nature, but it was almost too real for some players. Days ago, EA ditched plans to include a "Taliban" option in multi-player mode. Instead, players can choose to side with either American forces or the renamed "Opposing Force." The move came about a month after the game was banned from 49 Gamestop locations and all Post Exchanges on U.S. military bases worldwide due to the Taliban feature. Goodrich said in a blog post that EA got rid of the Taliban option out of respect for American soldiers and their families.

Former lawyer and video game violence activist Jack Thompson also tried to block the sale of the game. In a September letter to Secretary of Defense Robert Gates, Thompson said that the game shouldn't be sold "on the basis that it poses a demonstrable danger to our troops by providing a training tool for those who wish to kill them."

Despite the flack, the Afghanistan-based edition of the game saw the highest pre-orders in its history. It is available now for $59.95 for Xbox 360, Playstation 3, and the PC.

Atari Revives Star Raiders News

Decades-old shoot 'em up Star Raiders is set to get a modern makeover, publisher Atari has announced.

A handful of grey-haired gamers might remember the original first-person space shooter, which launched on the Atari 2600 in 1979. Yes, they made videogames back then.

The remake is being handled by Incinerator Studios, whose credits include Disney tie-in Cars.

Incinerator president Joel Goodman told Gamespot, "It isn't often that a developer gets to work with a genre-defining intellectual property, and Star Raiders is just that. Great games such as X-Wing and Wing Commander were influenced by this Atari classic.

"The original game had great tension when you warped into a sector not knowing what you would be facing, and at times you were immediately thrown into combat. Having to manage the flow of the game from the Galactic Map was a very unique and exciting experience."

Atari senior producer Jonathan Moses went on to say that this isn't the only retro update the publisher has in the pipeline.

"You're going to be seeing more of this from Atari in the near future. Along with some exciting new IP that we're working with, we're not ignoring our history. We're bringing back some of the classics in a way that makes them relevant now."

"It's an exciting time for Atari," he added.

A release date for Star Raiders has not yet been confirmed, but you'll be able to play it on PC, PlayStation 3 and Xbox 360.

Razer Announces 'Ironclad' Gaming Mouse Mat

Razer, a gaming peripheral manufacturer, announced its 'Ironclad' mouse mat - built to enhance your mouse's gliding capabilities.

The Ironclad is a metallic, specifically anodized aluminum gaming mat with a sandblasted surface that Razer claims makes for a smoother navigating and overall gaming experience. The mat accommodates for wide, sweeping motions with its 12.6 by 10.63 by 0.09-inch (LWH) dimensions.

Its base is made of rubber for stability and prevents the mat from moving during gaming sessions. The Ironclad also comes with a carrying case for portability to LAN parties. The case is also lined with foam and has a hard outer shell to protect it during accidental drops and spills.

The Razer Ironclad comes in white and has no decoration except for the Razer insignia. It's currently available from Razer's online store for $59.99.

Non-Retail Video Game Sales Hit $2.9 Billion

U.S. consumers spent up to $2.9 billion buying video games through mobile phones, social networks, downloads and subscriptions in the first half of the year, research firm NPD said on Friday.

The study marks the first time that NPD has released non-traditional video game sales figures and provides evidence that consumer spending on video games is 40 percent larger than it previously believed.

It estimated that non-traditional sales are at least $2.6 billion and as high as $2.9 billion, NPD said. The figures include used video game sales.

The move is, in part, defensive. NPD tracks and publishes monthly data on video game store sales, and has taken flak from video game executives for failing to account for new and increasingly popular ways of buying games.

NPD’s retail sales numbers have been less than pleasing to companies that make a living in the video game world. The research firm on Thursday reported that sales of video game software and equipment fell 8 percent in September.

Software sales fell 6 percent to $614 to million while hardware sales tumbled 19 percent to $383 million.

"This is an industry that is going through some pretty serious dramatic changes to its business model," said David McQuillan, NPD’s games president. "We have to change along with them to properly reflect the overall trends going on within the market."

Many customers are buying games through downloads or by visiting online social networks to play games offered by companies such as Zynga.

Apple Inc’s iPhone has also become a major gaming platform, with users buying games through the App Store.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Microsoft Releases Biggest-Ever Security Update

Microsoft released its largest-ever set of security patches Tuesday, fixing a total of 49 bugs in products such as Windows, Internet Explorer and Office.

There are 16 groups of patches (called updates) in total. Microsoft says that two of them - the Internet Explorer fix numbered MS10-071 and a Windows patch numbered MS10-076 - should get top priority. Microsoft thinks attack code is likely to be developed that will target bugs fixed by both of those updates.

NCircle Director of Security Operations Andrew Storms agrees that those two updates should be a top priority as they could be leveraged in a drive-by Internet attack. In this common type of attack, a hacker tricks the victim into visiting a Web page that takes advantage of the bug to install a malicious program on the victim’s machine.

The MS10-71 update fixes 10 Internet Explorer bugs. Two are rated critical, meaning they could be used in a drive-by. The MS10-076 update fixes a single

critical flaw in the Windows Embedded OpenType (EOT) Font Engine, used by Internet Explorer. The latest versions of Windows include a security technology called ASLR (address space layout randomization) which makes it harder to exploit that type of bug, Microsoft believes attackers are likely to develop attacks for older versions of the operating system such as Windows XP.

The two other top-rated updates are MS10-077, a fix for a bug in Microsoft's .Net Framework that affects 64-bit systems, and MS10-075, which fixes a critical flaw in the Microsoft Windows Media Player Network Sharing Service, used by Windows to share music files and other media over the network. This service is turned on by default with Windows 7 Home Edition, but a hacker would have to first be on the local network to launch an attack, Microsoft said.

Just because the other fixes are not rated critical does not mean they can be ignored. Symantec says 35 of the 49 bugs fixed on Tuesday could give hackers a way to run unauthorized software on a victim's machines, and Microsoft says attacks are likely to be developed that exploit some of the lower-rated issues as well.

In fact, one of Tuesday's updates - MS10-073; rated important by Microsoft - fixes a Windows XP bug that was leveraged by the creators of the Stuxent worm. Stuxnet is the first publicly known worm built to attack industrial systems and it has made headlines during the past weeks amidst speculation that it was designed to target nuclear systems in Iran.

UK Says It Gets Hit by 1,000 Cyber Attacks Monthly

British government computer networks are targeted by some 1,000 attacks a month, one of the country's top spies said in comments published Wednesday, adding that officials may consider investing in using cyberwarfare techniques to deter their online enemies.

GCHQ Director Iain Lobban told an audience of officials and academics in London that malicious software aimed at the U.K. had already caused significant disruption to the government's systems and that security officials were tracking the theft of intellectual property "on a massive scale."

"Cyberspace is contested every day, every hour, every minute, every second," Lobban said. "I can vouch for that from the displays in our own operations center of minute-by-minute cyber attempts to penetrate systems around the world."

Lobban described cyber security as an issue that "goes to the heart of our economic well-being and national interest" and made a catalog of warnings:

* He said there were more than 20,000 malicious e-mails on government networks each month 1,000 of them deliberately targeted.

* He said that one country, which he did not identify, had used cyber attacks on another in an attempt to coerce it.

* Online tax systems across Europe had been targeted by cybercriminals.

* The threat to the country's critical infrastructure was "real and

credible."

* E-crime was costing the British economy billions of pounds.

Lobban said that authorities were exploring a range of new options, including setting up a direct feed of information from infrastructure operators "so that we are aware of the attacks that they are seeing on their systems as they happen."

He also said government officials should also consider how to react to countries which deliberately attack Britain's electronic backbone - and whether "it may be possible to use military cyber capabilities for deterrent effect."

Still, he cautioned that there was no parallel to the paradigm of "Mutually Assured Destruction," the notion that nuclear-armed nations would not dare launch atomic attacks against each other for fear of provoking a devastating reaction. Cyber attacks, he said, took place "every day."

Lobban was speaking at the International Institute for Strategic Studies on Tuesday. The text of his speech has since been posted to the think tank's website.

Microsoft Will Look to Courts for Botnet Takedowns

Microsoft has seen a dramatic drop in the number of computers infected with Waledac, a piece of malicious software affiliated with a botnet that was once responsible for a massive amount of spam.

In the second quarter of this year, the company cleaned only 29,816 computers infected with Waledac, down from 83,580 computers in the first quarter of the year. Microsoft published the statistic in its latest biannual Security Intelligence Report released on Wednesday.

The drop in the number of infected machines shows the success of the legal action Microsoft took earlier in the year, said Adrienne Hall, general manager for Microsoft's Trustworthy Computing group.

Waledac was used to send spam and infect computers with fake antivirus software. It used a complicated peer-to-peer system to communicate with other infected machines.

Microsoft's legal moves against Waledac were unprecedented. The company was granted a rare ex parte temporary restraining order (TRO) to shut down malicious domain names that Waledac's controllers used to communicate with infected machines.

Going to court "gives you a blanket way to put on notice that you are going to look into the perpetrators," Hall said.

An ex parte TRO allows for an activity to be halted without notice to the bad actor and without granting that person a court hearing. In the case of Waledac, it meant that if the domain names were suddenly shut down, the botnet's operators wouldn't have much time to register new domains for their bots to call on to get new instructions.

Federal courts are reluctant to issue those kinds of orders because it may violate defendants' right to due process, according to Microsoft's report. But courts will grant an ex parte TRO if a judge is convinced the defendants may quickly reorganize and continue their bad activity. Microsoft was able to get two of those orders.

In other civil summons documents, Microsoft named 27 "John Does" who had registered the bad domains, which the company said provided the court "with an identifiable target for legal service while protecting the registrants' due process rights."

But most of the 276 domains used to control Waledac were registered through registrars in China. In another sign of Microsoft's diligence, the company researched how to craft an application for an ex parte TRO that also complied with Chinese law. It also researched how to serve those defendants in compliance with international treaties.

The international domain name registrants were served through the Hague Convention on Service Abroad, and all of the documents were sent to China's Ministry of Justice in addition to being published on a specific Web site.

The domains were shut down within 48 hours after the U.S. District Court for the Eastern District of Virginia granted the order. Last month, the court held a hearing on entering a default judgement against the unidentified defendants and transferring control of the domains to Microsoft. The company said in its report that a permanent injunction is pending.

"We think this has effectively dealt a blow to Waledac," Hall said.

While lawyers worked on the legal side, technical experts also attacked Waledac. Microsoft marshalled a team of computer security researchers who infiltrated Waledac's peer-to-peer control system. Once inside the botnet, they commanded infected machines to report to their own servers, cutting the cybercriminals off from their own botnet.

But while Waledac was stung, it still lives. The botnet comes in at No. 23 of the 25 most-detected botnet families, according to Microsoft's report, showing that even after extensive legal and technical efforts, botnets are difficult foes.

USA Is Still #1 In Botnets

We may not make a lot of things in the USA anymore, but we still lead the world in botnets by a large margin according to volume 9 of Microsoft's Security Intelligence Report, covering January through June of this year.

The main focus of the report is on botnets and Microsoft sees them as the core platform of malware, the engine that makes the Internet criminal enterprise run. And botmasters are getting more sophisticated: While we have historically thought of different kinds of malware (worms, trojans, spyware) separately, they are bring used together in bots. You might see password stealers used in addition to an IRCbot, for example.

But the bigger news is that this reports confirms some already established trends of decline in several negative factors: Software vulnerabilities,

industry-wide, continue to decline in numbers, but remain at high levels. Microsoft doesn't speculate about it, but I think the high numbers are due at least as much to large amounts of talent and money going into white hat research.

This being Microsoft, they have data on how much we're updating Windows and their other software, and the news there is good too. Consistent monthly use of Windows Update and other automated Microsoft update mechanisms (e.g. WSUS or Windows Software Update Services) is up substantially. These users should be far better protected against attack.

It's likely that this phenomenon is due to increased adoption of Windows 7 and, to a lesser extent, Vista, both of which make Windows Update and automatic application of updates the default behavior rather than a strong suggestion, as in XP SP3. The increased use of Windows Update also means more widespread runs of the Microsoft Malicious Software Removal Tool, which runs each time you run Windows Update. This month Microsoft added the Zeus trojan to the list of threats cleaned by the MSRT, which should deal a serious blow to a major botnet already in decline. The percentage of Vista systems needing an MSRT cleaning was 1/5 that of XP SP3 systems, and the percentage of Windows 7 systems 1/2 of Vista's.

Another major theme of the report is that malware is a world-wide phenomenon and problem and that any serious improvement in the situation will have to have an international basis. You can't just solve it in the US. Microsoft also repeats here their discussion of progress in collective defense and a "public health" model for Internet security.

Norton 360 Version 5 Enters Beta Testing

Symantec on Tuesday launched the free public beta test of Norton 360 version 5. The updated Norton 360 will incorporate all of the security enhancements introduced with Norton Internet Security 2011, but will also feature a redesigned user interface, faster tune-up, and a "revamped user backup experience."

Dan Nadir, Symantec's senior director of product management for consumer security, stated that the online backup component will have lower system impact, enhanced performance, and better communications with the user. He noted that the average amount of disk space for backup is growing right up to the 2GB limit.

"I used to say it's like a safe deposit box," said Nadir. "They store the really important stuff in case a fire burns up the PC and local backup. But people are doing more now."

Nadir reported a steady growth in the amount of data backed up per user and a smaller growth in average file size. He explained that in order to avoid open file problems Norton makes a copy of each file and backs up from the copy. "We've tweaked that for version 5 to use less resources. Backing up more data naturally takes longer, so we added better communication about backup status," he said.

Symantec's own research shows that the PC tune-up feature is more popular than expected. "We thought they would have rated backup more important," said Nadir, "but in fact they put tune-up above backup."

Users want a faster tune-up experience that helps them squeeze out every ounce of performance; version 5 will improve tune-up.

In conjunction with the Norton 360 beta, Symantec is releasing version 1.5 of Norton Power Eraser to its own separate beta test. Norton Power Eraser is a free tool designed to remove scareware and other persistent malware that may interfere with installation of ordinary security software. The most significant addition in version 1.5 is the ability to fine-tune detection by querying the huge Norton Insight online database.

Norton 360 version 5 beta is available now at www.norton.com/n360v5beta. Find Norton Power Eraser at http://security.symantec.com/nbrt/npe.asp. PCMag will evaluate and review Norton 360 after its release, expected this spring.

Comodo: 'We Beat Norton!'

Three weeks ago Comodo Security Solutions threw down the gauntlet. Responding to a Symantec product manager publicly who stated that free antivirus solutions can't protect as well as "more mature paid suites", Comodo chief executive Melih Abdulhayoglu challenged Symantec to an independent test to verify whether Comodo or Norton can protect users better.

Symantec reasonably responded that many independent tests already exist, and that Norton products are evaluated in almost all of them. Symantec suggested Comodo simply participate in those same tests.

Comodo immediately commissioned an evaluation by well-regarded testing lab AV-Test.org. The test measured each product's ability to prevent infestation by 30 brand-new zero-day threats. Comodo reports that their free antivirus scored 100 percent for "overall detection and protection" while Norton scored just 90 percent. "Not only are we as good," said Abdulhayoglu, "we're better at protecting the computer from completely new viruses and malware and it's FREE." A Comodo PR representative stated, "At this point, Comodo expects a public apology from Symantec".

A closer look at the detailed results reveals that there's more to the story. The test shows that both Comodo and Norton detected and warned about 100 percent of the threats, though Norton got just 90 percent for the "Overall Detection and Blocking Rate". Comodo didn't mention that for the "Overall Detection, Blocking and Removal (Cleaning) Rate" their product scored 53 percent to Norton's 80 percent.

Symantec's response pointed up the mixed nature of the test's results. "We are pleased to see that Norton detected a perfect 100 percent of threats [and] far outperformed the competitor in the comprehensive test, which proves whether a product can detect, block and remove threats Norton helps keep the system running clean, versus the competition which leaves a much higher percentage of malware on a user's system."

Symantec called into doubt the results of the false positive test, in which both products caused no false positive detections at all. "False positives can be a problem with programs that are overly aggressive in their attempt to achieve very high detection rates. Even though we received a perfect score of zero false positives in this test, Norton recommends and has excelled in real world testing with a larger sample

of legitimate applications that are balanced between popular, average and more unique applications."

Participation in the full range of independent lab tests can be expensive, especially when the product in question is free, but Comodo's presence in standard independent lab tests is slowly growing. Virus Bulletin included Comodo Antivirus 5.0 in their latest round of testing (though it did not achieve VB100 status).

Symantec's experts are reserving further comment until they've had the opportunity to review the test and its methodology in full. As things stand it doesn't seem likely Comodo will receive the requested public apology.

Trojan Forces Firefox to Save Your Passwords

A Firefox Trojan has been found to force the Internet browser to save user passwords and then use those passwords to create a new user account on the infected computer.

Most security researchers recommend that users tell Firefox not to remember their passwords, since saved ones are so easily extracted by malware.

The Trojan-PWS-Nslog malware discovered by security company Webroot, however, gets around user preferences altogether by actually deactivating the Firefox code that asks if it should save those passwords when the user logs into a secure site.

"Before the infection, a default installation of Firefox 3.6.10 would prompt the user after the user clicks the Log In button on a Web page, asking whether he or she wants to save the password," Webroot researcher Andrew Brandt explained in a blog post on Wednesday. "After the infection, the browser simply saves all login
credentials locally, and doesn't prompt the user."

Specifically, the Trojan adds a few lines of code and "comments out" other portions of code from the Firefox file called nsLoginManagerPrompter.js, with the result that all passwords get saved locally without any input from the user.

With that information, the Trojan creates a new account under the name "Maestro" on the infected computer. It then "scrapes information from the registry, from the so-called Protected Storage area used by IE to store passwords, and from Firefox's own password storage, and tries to pass the stolen information onward, once per minute," Brandt added.

The Web domain intended to receive the stolen data has already been shut down, but code inside the malware revealed the author's name and email address, which led Webroot to a Facebook page for a hacker based in Iran who provides a free keylogger creator tool targeting users of Microsoft Windows.

Webroot can easily identify and remove the Trojan from infected machines, it says. To fix the modified Firefox file, users should download the latest Firefox installer and install it over the existing installation. No bookmarks or add-ons will be lost in the process, Brandt said.

Mozilla’s Firefox ranks second in global browser market share, according to Net Applications, with 23 percent of the browser market in September. The first beta release of Firefox 4 for Android phones just debuted this week.

By default, Firefox does remember passwords. To tell it not to, go to the Tools menu and select Options. From there, open the Security tab and uncheck the appropriate box, Webroot advises.

Kensington Releases ClickSafe Keyed Laptop Lock

Kensington, a manufacturer of computer peripheral solutions, has announced a new laptop lock, the ClickSafe, to protect your PC from theft.

The ClickSafe utilizes your laptop’s case slot to place a metal anchor and lock the Kensington security device in place. Most laptops do have case slots, it’s just a matter of finding them. One laptop that, unfortunately, doesn’t have one is the MacBook Air.

Before you snap the ClickSafe in place with the anchor you will have to tether it to a table, chair, or other secure piece of furniture. This device won’t prevent people from otherwise viewing your files or even severing the carbon reinforced cable (61 inches), but it will deter or even slow down those who would try to steal your laptop.

I found it useful when going to Starbucks or Barnes & Noble to lock my laptop to the table, securing it while I retrieved a book or went to the bathroom. Unlocking the ClickSafe from your laptop requires a key. Kensington gives you two, but if you lose both without registering Kensington cannot replace your keys for you.

While a key lock seems more focused on business-end users, Kensington is planning on releasing a combination lock later next spring.

The Kensington ClickSafe Keyed laptop lock is available now from online retailers for $49.99.

Oracle Pledges Support for OpenOffice.org

Oracle sought to dispel any doubts about its commitment to OpenOffice.org on Wednesday, announcing its participation in the ODF Plugfest event in Brussels this week and talking up future development plans for the open source productivity suite.

Programmers and testers at the vendor "will continue developing, improving, and supporting OpenOffice.org as open source, building on the 7.5 million lines of code already contributed to the community," Oracle said in a statement. The company welcomes community contributions to the code base, it adds.

Oracle’s announcement follows last month’s move by some OpenOffice.org contributors to create an offshoot version of the suite under the name LibreOffice.

The group also formed a new organization called the Document Foundation, which released a "Next Decade Manifesto" on Wednesday. It lays out the group's philosophical principles, which include the rejection of "office productivity tools by monopoly suppliers" and the embrace of "an open and transparent peer-reviewed software development process where technical excellence is valued."

LibreOffice has support from a number of major vendors, including Google, Red Hat and Novell.

Last week, the group said a beta of LibreOffice had been downloaded more than 80,000 times and code contributions had already been made.

The group has said it has no intentions of creating a commercial product based on LibreOffice, although nothing stands in the way of vendors doing so.

Oracle itself sells Oracle OpenOffice, a product based on the OpenOffice.org code base that bundles in additional tools and extensions, including a Microsoft SharePoint connector.

The Document Foundation, which could not immediately be reached for comment Wednesday, has invited Oracle to join the organization and donate the OpenOffice.org brand name. An Oracle spokeswoman declined to comment on the status of that request.

Why Is Microsoft So Scared of OpenOffice?

Microsoft and its supporters have a long history of applying all kinds of FUD to any discussion of free and open source software. Whether it's Linux or other free alternatives to Microsoft's high-priced products, it seems no conversation can take place without the inevitable insinuations about higher total cost of ownership, lack of support, and other baseless fearmongering.

Such claims are, of course, nothing more than deliberately perpetuated myths designed to scare customers into Redmond's malware-infested arms, as I recently pointed out.

This week, however, we have a shining new example: A video on YouTube designed specifically to attack OpenOffice.org.

Could the sweat on Steve Ballmer's brow be any more evident?

It has been clear for some time now that free and open source software has Microsoft running scared. Last year, for instance, the company made plain the fact that it was worried about Linux's growing popularity and the detrimental effect that might have on the Windows empire.

And no wonder: Given the high prices, malware risks, and vendor lock-in associated with Microsoft's products, it has plenty to fear. Linux blows Windows away on both the desktop and the server - let's not even mention Microsoft's mobile track record - and open source productivity applications are apparently putting a serious dent in Microsoft's bottom line too.

Why else would the company bother to create this FUD-filled video? Titled "A Few Perspectives on OpenOffice.org," it features a series of "horror stories" from customers who tried the open productivity suite and purportedly suffered as a result.

"We originally installed Linux-based PCs running OpenOffice to save money in the short term," an unseen voice begins. "But we quickly found that the exorbitant cost and limited availability of support left us worse off."

Such concerns, of course, play upon the fourth and eighth myths described in my recent post on the topic, and are straight out of Microsoft's standard playbook. They also fly in the face of the fact that OpenOffice.org has set download records on new releases, and likely accounts for about 10 percent of the overall office suite market today. I guess all those millions of users are just suffering in silence!

Today, of course, there's not just OpenOffice.org - which Oracle recently pledged to continue supporting - but also LibreOffice, as well as a number of other business productivity alternatives. Amid all the increasing competition, one glaring question emerges: If Microsoft Office is so superior, better-supported and cheaper, then why the desperate attack video?

The answer is simple: Microsoft's products aren't superior, better-supported or cheaper. They're flaw-ridden, vulnerable and expensive, and they lock your company into a future of more of the same. Isn't it time you tried something better?

Rumors Have AOL and Equity Partners Circling Yahoo

It's a good time to hold Yahoo shares. The company's stock climbed in early trading Thursday on rumors that AOL and several equity firms might buy the Internet giant.

According to The Wall Street Journal, Silver Lake Partners and Blackstone Group LP are among the firms that have explored teaming with AOL to buy Yahoo, or even taking it private. The Journal said two or three other equity firms may also be interested in a buyout. However, Yahoo has reportedly not participated in any discussions.

Neither Yahoo, AOL or the known equity firms could immediately be reached for comment. But the speculation drove up Yahoo's shares more than nine percent in early Thursday trading. The company's stock has suffered since it refused a takeover bid from Microsoft in 2008 and continued to lose search market share to its search partner, Microsoft's Bing.

Greg Sterling, principal analyst at Sterling Market Intelligence, said the notion that AOL might try to do what Microsoft couldn't - bring Yahoo into its corporate structure - is totally speculative. Still, he shared some thoughts on what could be driving the rumors.

"Yahoo is undervalued and private equity firms want to potentially 'unlock' that value in several ways, including the sale of some assets, such as Alibaba," Sterling said. "There's also a scenario in which Yahoo goes private and gets out from under the glare of the stock market."

Tapping into private equity to exit the market would also reduce Yahoo's expenses in regulatory filings and perhaps enable the company to make some moves without tipping its hand to competitors. Yahoo could become leaner as a private company and reenter the public market stronger.

"An AOL-Yahoo merger - because they're very similar companies - also seems to make sense on paper and has been discussed before. But there are many challenges in making that a reality and executing after a merger," Sterling said. "But there's a broader sense in the market that Yahoo hasn't been able to turn around under [CEO Carol] Bartz and that it doesn't have the momentum it should - hence the vultures are circling."

Yahoo rejected Microsoft's $44.6 billion takeover bid - twice. Microsoft CEO Steve Ballmer sent what amounted to an ultimatum letter to Yahoo's board making it clear that Microsoft's goal in making "such a generous offer" was to create the basis for a speedy and ultimately friendly transaction.

Many analysts now are saying Yahoo made a colossal mistake in repeatedly snubbing Microsoft. But would merging with AOL be the right path for Yahoo? AOL acquired technology blog TechCrunch last month to beef up its content offerings. Yahoo would bring AOL a large content network to advertise against. But many analysts think it's unlikely that a merger would threaten dominant player Google.

Apple Hints at New Mac OS in Invitation to Media

Apple is inviting media to its Cupertino, Calif., headquarters for a Macintosh computer-related event on Oct. 20.

Apple Inc. is known for its secrecy about upcoming products. The invitation sent Wednesday offers no concrete details about the products to be announced. However, it does show an image of Apple's logo opening like a door to reveal a glimpse of a lion.

That's a clue that Apple plans to introduce a new version of Mac OS X, the operating system software that runs on the company's desktop and laptop computers. Apple calls its Mac computer operating system updates by names of large cats. The most up-to-date version is Snow Leopard. Previous versions include Leopard, Tiger and Panther.

Australia PM Backs Controversial Web Filter

Australian Prime Minister Julia Gillard Tuesday renewed her backing for a controversial Internet filter, saying it was driven by a "moral question".

The proposed filter will block access to material such as rape, drug use, bestiality and child sex abuse, and will be administered by Internet Service Provider companies.

However, web giants like Google, Yahoo! and Microsoft have slammed the initiative as setting a precedent for censorship, while cyber-activists have hit government websites with a targeted hacking campaign.

"My fundamental outlook is this: it is unlawful for me as an adult to go to a cinema and watch certain sorts of content, it’s unlawful and we believe it to be wrong," Gillard said in a press club address.

"If we accept that then it seems to me that the moral question is not changed by the medium that the images come through."

The plan, which has also drawn concern from the US State Department, was put on hold pending a content review in July as national elections loomed.

Angry user groups have launched an online campaign accusing the government of censorship, likening the proposed system to firewalls operating in China and Iran.

Concerns have also been raised about the filter’s impact on Internet speeds and the methods through which restricted content would be determined.

Gillard said how to set up the filter "is more complicated, but the underpinning moral question is, I think, exactly the same".

A review of what material should be excluded by the filter is expected to take at least 12 months.

Pennsylvania School District Settles Webcam Spying Case for $610K

A Pennsylvania school district accused of remotely activating webcams on school-issued laptops has reached a settlement with two students who sued the district over the breach.

The Lower Merion School District will pay a total of $610,000 to settle cases filed by students Blake Robbins and Jalil Hassan. The move comes after the district’s insurance carrier, Graphic Arts, agreed to cover more than $1.2 million in fees and costs associated with the litigation.

At issue are school-issued Mac laptops provided to 2,300 students at Harriton High School. Unbeknownst to those students and their parents, the laptops were equipped with tracking software that could remotely activate the computer’s webcam to take photos of the user, as well as capture screen shots. It was intended as a means to locate lost or stolen laptops, but was apparently activated in more questionable circumstances as well.

The tracking software came to light when Robbins, a student at the high school, was allegedly called into the assistant principal’s office and accused of taking drugs. The evidence was reportedly screen shots of Robbins from the school-issued laptop that appeared to show him taking pills. Robbins said he was actually eating candy.

His parents filed suit against the school district in February. Several months later, Hassan was informed that the software on his computer had also been activated, capturing 469 pictures from the webcam and 543 screen shots over the course of several months. Since he was 18, Hassan then filed his own lawsuit.

The $610,000 deal includes $10,000 for Hassan and a $175,000 payout that will be placed in a trust for Robbins. The district will also pay

$425,000 in legal fees.

"We believe this settlement enables us to move forward in a way that is most sensitive to our students, taxpayers and the entire school district community," board president David Ebby said in a statement.

In late August, the U.S. Attorney's Office announced that it would not bring criminal charges against the district. No one involved in the case had criminal intent, U.S. Attorney Zane David Memeger said at the time.

"That was an important moment for us; it confirmed the results of an independent investigation and the District's own initial findings," Ebby said Monday.

The school district has since apologized and admitted that it should have informed students and parents about the software. An updated school policy now requires the district to get a student's permission before activating the monitoring software.

The district chose to settle because a trial would have been costly and distracting, Ebby wrote. The district also "wanted to be sensitive to the welfare of the student involved in the case," though he went on to essentially say that the lawsuits have been a major waste of taxpayer dollars.

"I want you to know that had concerns about privacy been brought to the Board without legal action, they would have been addressed effectively and immediately as well, without additional costs to taxpayers," Ebby said.

UK Police Force Publishes All Incidents to Twitter

From stolen cars to suspicious smells, one of Britain's biggest police forces is tweeting every incident it deals with over a 24 hour-period to prove a point.

The online Twitter campaign aims to show the pressures that police are under as British officials prepare for deep budget cuts.

"The reality of police work is that although crime is a big part of what we do, we do much else besides," Chief Constable Peter Fahy of Manchester said in a message posted to YouTube. "We're very much the agency of last resort, and a big part of our workload is related to wider social problems of alcohol, drugs, mental health and people having problems with their relationships."

The project, which began at 5:00 a.m. Thursday, has already racked up more than 1,300 different incidents. Among the first tweets: An alert about a stolen vehicle thought to be headed for Manchester, the arrest of an aggressive shoplifter, and a report that "a man appears asleep at bus stop."

Greater Manchester Police is one of the country's largest police forces, responsible for a 500-square-mile (1,300-square-kilometer) area centered on Manchester, which competes with Birmingham for the title of England's second city.

Although Manchester has seen some high-profile crimes - including international terrorism cases - most of Thursday's calls spoke of the daily

grind of police work.

Many tweets covered domestic incidents, traffic accidents, stolen cars and missing people. There were calls about animals, complaints about a man urinating against a school wall, and a report of someone smoking on an incoming flight to Manchester Airport.

There were also dozens of false alarms.

In one incident, officers were sent to a bridge where a man was reportedly seen dangling a baby over the edge. In fact, he'd been carrying his dog in his arms because the animal was afraid of bridges.

The Twitter feed was choked with reports of children who had dialed police while playing with their parents' cell phones, as well as a host of nuisance calls.

"Confused man reporting his TV not working," one incident report stated. "Man calls to say locked out of house. Wants police to break in for him," another said. One woman called police because a video of her had been posted to YouTube.

Manchester police said the tweets were being sent by a team of people from its corporate communications department, along with two force inspectors. Incidents would not be tweeted if their publication threatened anyone's safety, a spokeswoman said.

For technical reasons, the police updates were being published across three different Twitter feeds. The project is to run until 5 a.m. Friday.

=~=~=~=